REMARKS

Responsive to the Office Action mailed July 26, 2006, Applicants provide the following. Claims 4 and 50 have been amended into independent form (fees for two additional independent claims are provided herewith). Claims 13, 24, 35, 60, 69, and 79 were previously canceled. No new claims have been added. Eighty-seven (87) claims remain pending in the application: Claims 1-12, 14-23, 25-34, 36-59, 61-68, 70-78, and 80-93. Reconsideration of claims 1-12, 14-23, 25-34, 36-59, 61-68, 70-78, and 80-93 in view of the amendments above and the remarks below is respectfully requested.

Initially, Applicants acknowledge with appreciation that dependent claims 4-7 and 50-55 have been indicated to include allowable subject matter. Applicants also appreciate the Examiner's willingness to schedule a telephone interview to discuss the office action; however, regret that due to injury, this interview was canceled. Applicants kindly ask that the Examiner contact the undersigned at (858) 552-1311 when this response is received to discuss.

Allowable Subject Matter

1. Claims 4-7 and 50-55 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form. Claims 4 and 50 have been amended into independent form; thus, it is respectfully submitted that all of claims 4-7 and 50-55 should be allowed independent of the remarks presented below.

Claim Rejections - 35 U.S.C. §102

2. Claims 1-3, 8-12, 14-23, 25-34, 36-49, 56-68, 70-78 and 80-93 are rejected under 35 U.S.C. § 102(e), as being allegedly anticipated by Abdo et al (U.S. Publication No. 2002/0141591). This rejection is respectfully traversed and reconsideration is requested.

As set forth at M.P.E.P. § 2131, a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference.

All pending independent claims variously require the transmission/reception of a message containing a first encryption key over a wireless network, the message encrypted with a

second encryption key. For example, independent claim 1 recites "an encryption unit configured to encrypt a message containing the first encryption key, the message encrypted with the second encryption key" and "a radio configured to transmit the message over a wireless network". Independent claim 47 recites "a radio configured to receive a message over a wireless network from a host..., the received message encoded with the first encryption key and containing a second encryption key". It is respectfully submitted that Abdo et al. do not expressly or inherently disclose this feature as variously recited, nor would render obvious this feature.

That is, Abdo et al. describe a system and method for securely connecting wireless peripheral devices, such as a wireless keyboard, to a host system, such as a personal computer (See Abstract). Referring to the Summary section as indicated by the Examiner, Abdo et al. clearly provide a technique in which the wireless peripheral device is provided an encryption key generated by the host system *without having to directly transmit the encryption key* to the wireless peripheral (see paragraph [0010], emphasis added). Abdo et al. also provide for the validation of the secure link, again, *without having to transmit an encryption key* between the wireless peripheral and the host system (see paragraph [0010], emphasis added). This is also confirmed in paragraph [0071].

Specifically, referring to the detailed description of the Abdo et al. document, initially the user requests a secure connection (see paragraphs [0054]-[0057]) between a wireless peripheral (wireless keyboard 115) and a host adapter or receiver 111. The receiver 111 is coupled by wireline to a host computer 102 (see FIG. 1). Next, the receiver 111 generates an encryption key and a transmission sequence, the transmission sequence having a first half representing the encryption key and a second half representing a confirmation sequence (see paragraph [0058]). This encryption key and transmission sequence is sent by the receiver 111 to the host device 102 by wireline (see paragraph [0058]). Next, the host computer 102 causes the transmission sequence to be displayed on a display unit 103 with instructions for the user to type the viewed sequence into the keyboard 115 (see paragraph [0058]). The user then types the sequence into the keyboard 115, which the keyboard uses to reconstruct the encryption key (see paragraph [0059]). Since the typed sequence input into the keyboard 115 represents the encryption key, this "prevents the encryption key from being directly transmitted from the wireless keyboard 115 to the host device over the connection" (see paragraph [0060]). Once the encryption key is reconstructed, the keyboard 115 switches to an

encryption mode (see paragraph [0061]). The computer 102 causes the confirmation sequence to be displayed on the display unit 103 and the user then types the confirmation sequence into the keyboard 115 (see paragraph [0061]). The keyboard 115 encrypts the confirmation sequence using the encryption key and wirelessly sends the encrypted confirmation sequence back to the receiver 111 (see paragraph [0061]). The receiver 111 and host computer 102 decrypt the confirmation sequence using the encryption key (which is already present at the receiver 111 since it was generated by the receiver 111) and use the confirmation sequence to verify that the keyboard 115 is using the same encryption key as the receiver 111 (see paragraph [0062]). Again, this connection method provides an encryption key generated by the host system to the wireless peripheral *without having to directly transmit the encryption key* to the wireless peripheral (see paragraphs [0010] and [0071]).

Thus, it is clear that no where do Abdo et al. disclose or suggest the transmission/reception of a message containing a first encryption key over a wireless network, the message encrypted with a second encryption key, as is variously recited in all independent claims. Specifically, at no time do Abdo et al. transmit/receive a message containing an encryption key over the wireless network.

Thus, since Abdo et al. do not disclose, either expressly or inherently, or even suggest that recited in independent claims 1, 12, 23, 34, 47, 58, 67 and 76, Abdo et al. do not anticipate any of claims 1-3, 8-12, 14-23, 25-34, 36-49, 56-68, 70-78 and 80-93, nor would Abdo et al. render obvious any of these claims. Thus, it is respectfully submitted that the rejection of claims 1-3, 8-12, 14-23, 25-34, 36-49, 56-68, 70-78 and 80-93 is overcome and should be withdrawn.

CONCLUSION

Applicants submit that the above remarks place the pending claims in a condition for allowance. Applicants also request that the Examiner contact the undersigned by telephone at (858) 552-1311 to discuss the rejection and arguments presented herein. Therefore, a Notice of Allowance is respectfully requested.

Respectfully submitted,

Dated: December 27, 2006 /Scott J. Menghini/

Scott J. Menghini
Reg. No. 42,880
Attorney for Applicants
(858) 552-1311

Address all correspondence to:
FITCH, EVEN, TABIN & FLANNERY
120 So. LaSalle Street, Ste. 1600
Chicago, IL 60603